UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/804,835	03/19/2004	Ramarathnam Venkatesan	MS1-1286US	7125

22801 7590 04/17/2008

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
PERUNGAVOOR, VENKATANARAY	
ART UNIT	**PAPER NUMBER**
2132	
MAIL DATE	**DELIVERY MODE**
04/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/804,835	VENKATESAN ET AL.	
	Examiner	Art Unit	
	Venkat Perungavoor	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *14 March 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments filed 3/14/2008 have been fully considered but they are not persuasive.

The Applicant argues that the office has failed to show the vector being based on predefined hashing function of message.

> Tsuji discloses the vector being based on hash see Page 468 “Step 4” and further it being based on a message see Page 467 “I. Introduction".

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 102

Claims 1-3, 6-8, 11-15, 18-19, are rejected under 35 U.S.C. 102(b) as being anticipated by NPL to Tsujii.

Regarding Claim 1, 13, Tsujii discloses the obtaining message M see Page 467- II. El Gamal’s Public-Key Cryptosystem-<Encryption>; defining a vector to $v_1 \ldots v_n$ based upon a predefined first hashing function of the message see Page 468 –(12); calculating a private key α in accordance with equation $\sum_{1 \le i \le n} v_i \alpha_i \bmod m$ see Page 468 item 16; producing a signature S in accordance with the equation $S = \alpha H_2(M)$, where $H_2(M)$ is a predefined second hashing function see Page 470-(39).

Regarding Claim 2, 11, 14, Tsujii discloses the results of indicating message and signature(M,S) see Page 471-(55).

Regarding Claim 3, 15, Tsujii discloses the mapping of third hashing into an integer range see Page 469- Second Column 2- “An arbitrary..”

Regarding Claim 6-7, 18-19, Tsujii discloses the hashing in –1 and 1 see Page 469 Second full paragraph “An abitrary…”

Regarding Claim 8, 12, Tsujii discloses the output device and medium see Page 471 “Enhancement of Security and Processing Cost”.

Claim Rejections - 35 USC § 103

Claims 4-5, 9-10, 16-17, 20-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over NPL to Tsujii in view of NPL2 to Chen.

Regarding Claim 4-5, 9-10,16-17, 22, 30,Tsujii disclose the discrete logs of points on an elliptic curve and tate-weil pairings. However, Chen discloses the discrete logs of points on an elliptic curve and tate-weil pairings see Page 9 14¶ “Suppose that there are…”.It would be obvious to one having ordinary skill in the art at the time of the invention to include the discrete logs of points on an elliptic curve and tate-weil pairings in the invention of Tsujii in order to unique session keys.

Regarding Claim 20, 27, 28, 35, 37, Tsujii discloses the obtaining message M and signature(M,S) see Page 471-(55) & Page 467- II. El Gamal's Public-Key Cryptosystem-<Encryption>; defining a vector to $v_1 \ldots v_n$ based upon a predefined first hashing function of the message see Page 468 –(12); calculating a private key α in accordance with equation $Q= \sum_{1 \le i \le n} v_i Q_i \bmod m$ see Page 468 item 16. But does not disclose the calculating the point on an elliptic curve, comparing of pair (P, S) and pair (Q, H_2(M)) and indicating results of comparing. However, Chen discloses the point on an elliptic curve(Page 3 1¶), comparing of pair (P, S) and pair (Q, H_2(M)) and indicating results of comparing see (Page 1¶ "At the conclusion…"). It would be obvious to one having ordinary skill in the art at the time of the invention to include the calculating the point on an elliptic curve, comparing of pair (P, S) and pair (Q, H_2(M)) and indicating results of comparing in the invention of Tsujii in order to have an authentication system/key verification system as taught in Chen see Page 10 9¶ "The method used …".

Regarding Claim 21, 29, 36, Tsujii discloses the results of indicating message and signature(M,S) see Page 471-(55).

Regarding Claim 23-26, 31-34, Chen discloses the comparing not a match then the repeating the defining, calculating, modifying and comparing see Page 10 7¶ ("The proof…").

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Venkat Perungavoor whose telephone number is (571)272-7213. The examiner can normally be reached on 8:30-5:00.
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/V. P./
Examiner, Art Unit 2132
April 8, 2008

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132